IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

AMANDA JOHNSEN, individually and on behalf of all others similarly situated; Plaintiff, v. **AMERICAN WATER WORKS COMPANY, INC.,** Defendant.	Case No.: 1:24-cv-9752 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff Amanda Johnsen ("Plaintiff") brings this Class Action Complaint against American Water Works Company, Inc. ("American Water" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information (collectively, "PII" or "Private Information"). Now, the PII is in the hands of cybercriminals who will use Plaintiff's and the Class's PII for an unlimited time.

2. Defendant American Water Works Company, Inc. is a Delaware Corporation. It employs more than 6,500 dedicated professionals who provide regulated and market-based drinking water, wastewater, and other related services to an estimated 14 million people in 24

states.[1]

3. In a 8-K filing with the SEC on October 7, 2024, Defendant identified it was subject to a cyberattack in or about October 03, 2024 (the "Data Breach").[2] Defendant is still investigating the Data breach and has not yet sent notice to its customers. However, Plaintiff and the Class have already been locked out of their water utility accounts, which include Plaintiff's personal information such as her private bank account information. Plaintiff has already felt the effects of the cyberattack as her personal bank account had an attempted intrusion several days after the October 3rd attack on Defendant.

4. Plaintiff brings this class action lawsuit on behalf of herself and those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information was likely accessed by an unknown third party and precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Personal Information was a known risk to Defendant and thus Defendant was on notice that failing to take steps necessary to secure the Personal Information from those risks left that information in a dangerous condition.

6. Because of the Data Breach, Plaintiff and Class Members suffered ascertainable

[1] https://amwater.com/corp/about-us/corporate/#:~:text=We%20are%20the%20largest%20and,have%20an%20experienced%20leadership%20team. (last viewed October 10, 2024).
[2] https://www.techtarget.com/searchsecurity/news/366612830/American-Water-discloses-breach-utilities-unaffected (last viewed October 10, 2024).

losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

7. By obtaining, collecting, using, and profiting from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits its systems, which contain Plaintiff and Class Member's Private Information, was attacked.

8. The exposed Private Information of Plaintiff and Class Members can-and likely will-be sold on the dark web. Indeed, Plaintiff's and Class Members' Private Information has likely already been published on the dark web.

9. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers—the gold standard for identity thieves.

10. This Private Information was compromised because of Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant has yet to contact affected individuals or any state attorney generals.

11. Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their lifetimes.

12. Plaintiff brings this action on behalf of all persons whose Private Information was compromised because of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private

Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury because of Defendant's conduct. These injuries include:

(i) lost or diminished value of Private Information;

(ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

(iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, lost time; and

(iv) the continued and exacerbated to their Private Information which:

a. remains unencrypted and available for unauthorized third parties to access and abuse; and

b. may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded. Defendant further disregarded their rights by failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures for the encryption of data, even for internal use.

15. Because of the Data Breach, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

16. Plaintiff Amanda Johnsen is a Citizen of Birdsboro, Pennsylvania and intends to

remain there throughout this litigation.

17. Defendant American Water Works Company, Inc. is a Delaware Corporation. American Water's principal place of business is located at 1 Water Street, Camden, New Jersey, 08102. American Water's registered agent is The Corporation Trust, located at 1209 Orange Street, Wilmington, County of New Castle, Delaware 19801.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff is a citizen of Pennsylvania, and presumably many of Defendant's customers have different citizenship from Defendant like Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has personal jurisdiction over Defendant because American Water operates, and is headquartered, in this District and conducts substantial business in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(l) because a substantial part of the events giving rise to this action occurred in this District. Defendant is also based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members from and/or in this District.

FACTUAL ALLEGATIONS

The Data Breach

21. Defendant claims that an unauthorized party accessed Defendant's business application on October 03, 2024 and acquired Private Information. On information and belief, the private information at issue includes name, address, phone number, social security number and financial account information.

22. On information and belief, as American Water has not said otherwise, Plaintiff's

and the Class Members' PII remain in the hands of the cybercriminals to date.

23. The Private Information accessed and exfiltrated was likely not encrypted because if properly encrypted, then cybercriminals would not have acquired and accessed Plaintiff's and Class Members' Private Information.

24. Defendant had obligations under contract, industry standards, and common law to reasonably protect and safeguard Plaintiff's and Class Members' Private Information from unauthorized access.

25. Defendant agreed to and undertook legal duties to maintain the protected Private Information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

26. The private information held by Defendant in its computer system and network included the Private Information of Plaintiff and Class Members.

27. By obtaining, collecting, using, and profiting from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

28. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

29. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosure of this Private Information.

30. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information, which includes Social Security numbers and financial account information, information that is static, does not change,

and can be used to commit myriad financial crimes.

31. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their Private Information.

32. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

33. On information and belief, Defendant maintained the Private Information of Plaintiff and Class Members, including, but not limited to, names, addresses, phone numbers, social security numbers, and financial account information.

34. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of Private Information.

35. Because of Defendant's failure to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, upon information and belief, cybercriminals infiltrated Defendant's systems and stole Plaintiff's and Class Members' Private Information.

36. The unencrypted PII of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

37. Defendant admitted that Private Information potentially impacted in the Data Breach contained name, driver's license, credit card number and expiration date, date of birth,

phone number and/or other personal information.

38. Because Defendant failed to properly protect safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Plaintiff's and Class Members' Private Information stored on Defendant's system.

Plaintiff Amanda Johnsen's Experience

39. Plaintiff Amanda Johnsen has been a customer of Defendants for several years. In order to access her water services through Defendant, Plaintiff had to provide her PII, including her personal financial account information for billing purposes.

40. Plaintiff provided her Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law.

41. On or around October 03, 2024, Defendant's network underwent a cyberattack and Plaintiff's Private Information was involved in the Data Breach.

42. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

43. Plaintiff stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

44. Because of the Data Breach, Defendant directed Plaintiff to take certain steps to protect her Private Information and otherwise mitigate her damages.

45. Because of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

46. Even with the best response, the harm caused to Plaintiff cannot be undone.

47. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information-a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

48. Even worse, Plaintiff had an actual attack on her private banking accounts days after the cyberattack occurred on American Water. It was the same bank account that she provided to American Water for billing their services. Now, Plaintiff's entire financial security has been compromised by American Water's failed security.

49. Plaintiff has suffered imminent and impending injury arising from the exacerbated of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

50. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

The Data Breach was Foreseeable.

51. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[3]

52. Defendant's data security obligations were particularly important given the global rise in cyberattacks and/or data breaches preceding the date of the breach. In 2023, a record 3,205

[3] *See* How to Protect Your Networks from **RANSOMWARE**, at 3, *available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view* (last accessed Oct. 10, 2024).

data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100% increase from 2019.[4]

53. Considering recent high profile cybersecurity incidents across the country, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

54. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so that they are aware of, and prepared for, a potential attack.[5]

55. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Value of Private Information

56. The Private Information of individuals remains of high value to criminals, as shown by the prices they will pay through the dark web. Many sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[7] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[8]

57. For these reasons, the information compromised in the Data Breach is far more

[4] https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited Oct. 10, 2024).
[5] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbisecret-service-wam-of-targeted-ransomware (last accessed Oct. 10, 2024).
[6] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at:* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Oct. 10, 2024).
[7] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at:* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Oct. 10, 2024).
[8] *In the Dark*, VPNOverview, 2019, *available at:* https://vpnoverview.com/privacy/anonymous-browsing/tor/ (last accessed Oct. 10, 2024).

valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

58. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information... [is] worth more than 10x on the black market."[9]

59. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, financial services, and housing or even give false information to police.

60. The fraudulent activity resulting from the Data Breach may not come to light for years.

61. Drug manufacturers, device manufacturers, pharmacies, hospitals, and financial service providers often purchase PII on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' insurance premiums.

62. According to account monitoring company LogDog, PII sells for $50 and up on the Dark Web.[10]

63. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

[9] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers,* IT World, (Feb. 6, 2015), *available at: https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html* (last accessed Oct. 10, 2024).

[10] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals,* Naked Security (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/ (last accessed (Oct. 10, 2024).

from data breaches cannot necessarily rule out all future harm.[11]

64. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members because of a breach.

65. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

66. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of individuals detailed, personal information and thus the significant number of individuals who would be harmed by the exposure of the unencrypted data.

67. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and class Members.

68. As a condition of providing employment, Defendant requires that its employees entrust it with Private Information.

69. By obtaining, collecting, using, and profiting from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at: https://www.gao.gov/assets/gao-07-737.pdf* (last accessed Oct. 10, 2024).

70. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

71. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendant Acquires, Collects, and Stores the Private Information of Plaintiff and Class Members

72. Defendant acquired, collected, and stored the Private Information of Plaintiff and Class Members.

73. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

74. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Failed to Properly Protect Plaintiff's and Class Members' Private Information

75. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for some time.

76. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

77. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

78. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

79. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

80. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls-including file, directory, and network share permissions-with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[12]

81. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling

[12] *Id.* at 3-4.

or a different domain (e.g., .com instead of .net) ....

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters-and keep them updated-to reduce malicious network traffic.[13]

82. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

[13] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last accessed Oct. 10, 2024).

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection; and
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[14]

83. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all the above measures to prevent and detect cyberattacks.

84. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

85. As the result of computer systems needing security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff' and Class Members' Private Information.

86. Because Defendant failed to properly protect safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access Defendant's

[14] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Oct. 10, 2024).

network, and access Defendant's database and system configuration files.

87. Specifically, Defendant admits that on or around May 07 and June 20, 2024, an unauthorized party accessed Defendant's network and deleted databases and system configuration files.

88. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all the above measures to prevent and detect cyberattacks.

89. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

90. As the result of computer systems needing security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

Defendant Failed to Comply with FTC Guidelines

91. The Federal Trade Commission ("FTC") has promulgated Many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should influence all business decision-making.

92. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the private information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security

problems.[15]

93. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

94. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

95. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect private data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section *5* of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

96. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section *5* of the FTC Act, 15 U.S.C. § 45.

97. Defendant was always fully aware of its obligation to protect the PII of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result

[15] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

from its failure to do so.

Defendant failed to Comply with Industry Standards

98. As shown above, experts studying cyber security routinely identify professional service companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

99. Several best practices have been identified that at a minimum should be implemented by professional service providers like Defendant, including, but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, antivirus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

100. Other best cybersecurity practices that are standard in the professional services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

101. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, without limitation, PR.AC-I, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-I, PR.DS-1, PR.DS-5, PR.PT-I**,** PR.PT-3, DE.CM-I, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

102. The foregoing frameworks are existing and applicable industry standards in the professional services industry, and Defendant failed to comply with these accepted standards,

thereby opening the door to and causing the Data Breach.

Defendant's Negligent Acts and Breaches

103. Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect the Personal Information of Plaintiff and the Class;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train employees in the proper handling of emails containing how the cyberattackers were able to first access Defendant's networks, and to and maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(l);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(l)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(l)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section *5* of the FTC Act; and

n. Failing to adhere to industry standards for cybersecurity.

104. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Personal Information by allowing/providing unsecured and unencrypted Personal

Information to Defendant which in turn allowed cyberthieves to access its IT systems. This is due to Defendant's outdated antivirus and malware protection software needing security updating, its inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and its other failures to maintain its networks in configuration that would protect against cyberattacks like the one here.

105. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Because of Defendant's Failure to Safeguard Private Information, Plaintiff and the Class Members have Experienced Substantial Harm and Will Face Significant Risk of Continued Identity Theft.

106. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

107. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, financial account information, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

108. Because of Defendant's failures to prevent-and to timely detect-the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

109. Stolen PII is one of the most valuable commodities on the criminal information black market According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

110. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

111. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

112. One such example of criminals using PII for profit is the development of "Fullz" packages.

113. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

114. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

115. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims, and the numbers are only rising.

116. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good" Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

117. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

118. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

119. Further complicating the issues faced by victims of identity theft, data thieves may

wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

120. The Federal Trade Commission ("FTC'') has also recognized that consumer data is a new and valuable form of currency.

121. The FTC has issued many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed;

(4) limiting administrative access to business systems;

(5) using industry-tested and accepted methods for securing data;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function properly;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.

122. According to the FTC, unauthorized PII disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[16] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

[16] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited October 10, 2024).

123. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Plaintiff's and Class Members' Damages

124. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

125. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant places the burden on Plaintiff and Class Members by requiring them to expend time signing up for that service rather than automatically enrolling all victims of this Data Breach.

126. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

127. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

128. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, financial or medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

129. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

130. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

131. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

132. Defendant provided no compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

133. Plaintiff and Class Members have been damaged by the compromise of their Personal Information in the cyber-attack. Moreover, Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

134. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out- of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their

name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security number; financial, medical, and bank accounts; and credit reports for unauthorized activity for years to come.

135. Moreover, Plaintiff and Class Members have an interest in ensuring that their Personal Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Personal Information is inaccessible online and that access to such data is password protected.

CLASS ALLEGATIONS

136. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated under Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

137. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach of Defendant occurring on or about October 3, 2024 (the "Class").**

138. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; all federal, state, or local governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

139. Plaintiff reserves the right to modify or amend the definition of the proposed classes

before the Court determines whether certification is appropriate.

140. Numerosity, Fed R. Civ. P. 23(a)(l): Class Members are so Many that joinder of all members is impracticable. Upon information and belief, Defendant has over 14 million customers whose Private Information may have been improperly accessed in the Data Breach,[17] and each Class is apparently identifiable within Defendant's records.

141. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

[17] https://www.kxan.com/business/press-releases/cision/20241010DC28092/privacy-alert-american-water-under-investigation-for-cyberattack-and-data-breach-potentially-affecting-14-million-customers/ (last viewed October 11, 2024).

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages because of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution because of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

142. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised because of the Data Breach, because of Defendant's misfeasance.

143. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged here apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct toward the Class as a whole, not on facts or law applicable only to Plaintiff.

144. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

145. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged here; it will permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

146. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

147. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

148. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

149. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

150. And Defendant has acted or refused to act on grounds generally applicable to the Classes and thus final injunctive or corresponding declaratory relief for the Class Members is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

151. Likewise, issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing

to safeguard the Private Information of Plaintiff and Class Members; and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief because of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Putative Rule 23 Class)

152. Plaintiff and the Class repeat and re-allege every allegation as if fully set forth herein.

153. Plaintiff and the Class entrusted Defendant with their Private Information.

154. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

155. Defendant knows about the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

156. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

157. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class

Members in Defendant's possession was adequately secured and protected.

158. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under regulations.

159. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

160. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

161. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

162. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly given Defendant's inadequate security practices.

163. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

164. Defendant's own conduct created a foreseeable risk of harm. to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach asset forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

165. Plaintiff and the Class had no ability to protect their Private Information that was

in, and possibly remains in, Defendant's possession.

166. Defendant was able to protect against the harm suffered by Plaintiff and the Class because of the Data Breach.

167. Defendant had and continue to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Info by third parties.

168. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

169. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

170. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

171. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

172. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

173. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent

dissemination of Private Information.

174. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information it was no longer required to retain under regulations.

175. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

176. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

177. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

178. Additionally, Section *5* of the FTC Act prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

179. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as detailed herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result

to Plaintiff and the Class.

180. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

181. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

182. The harm attributable to the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

183. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiff and the Class.

184. As a direct and proximate result of Defendant' negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

185. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

186. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have a right to recover actual, consequential, and nominal damages.

COUNT II
NEGLIGENCE PER SE
(On behalf of Plaintiff and the Putative Rule 23 Class)

187. Plaintiff and the Class repeat and re-allege every allegation as if fully set forth herein.

188. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

189. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

190. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

191. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff

and Class Members, Plaintiff and Class Members would not have been injured.

192. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

193. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered an injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Putative Rule 23 Class)

206. Plaintiff and the Class repeat and re-allege every allegation as if fully set forth herein.

207. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if its data had been breached and compromised or stolen.

208. In its Privacy Policy, Defendant represented that it would not disclose Plaintiff and Class Members' Private Information to unauthorized third parties.

209. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

210. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of

Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that their personal information was compromised because of the Data Breach.

211. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

212. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have a right to recover actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Putative Rule 23 Class)

213. Plaintiff and the Class repeat and re-allege every allegation as if fully set forth herein.

214. This Count is pled in the alternative to Count III herein.

215. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information.

216. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

217. Rather than provide a reasonable level of security that would have prevented the

Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by using cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

218. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

219. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

220. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

221. Plaintiff and Class Members have no adequate remedy at law.

222. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession and (vii) future

costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiff and Class Members.

223. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

224. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

a. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

c. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including, but not limited to, an order:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

   iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

   iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employee's compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the

threats that they face because of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

d. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Any other relief that this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands this matter be tried before a jury.

Date: October 10, 2024,

Respectfully submitted,

BROWN, LLC
_/s Nicholas Conlon
Nicholas Conlon (NJ Bar ID # 34052013)
nicholasconlon@jtblawgroup.com
Jason T. Brown (NJ Bar ID # 035921996)
jtb@jtblawgroup.com
111 Town Square Place, Suite 400
Jersey City, NJ 07310
T: (877) 561-0000
F: (855) 582-5297

EKSM, LLP
Jarrett L. Ellzey*
Texas Bar No. 24060864
jellzey@eksm.com
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEYS FOR PLAINTIFF
(* denotes *pro hac vice* forthcoming)